Mapping ISO/IEC 27001:2005 -> ISO/IEC 27001:2013

Carlos Bachmaier – http://excelente.tk/ - 20140218

2005		2013	
In 2005		In 2013	
0	Introduction		
0		0	
1.2	Application		
1.2		1	Scope
		1	
		6.1.3	Information security risk treatment
		6.1.3 d	d)
4	Information security management system		
4.1	General requirements		
4.1		4.4	Information security management system
		4.4	
		4	Context of the Organization
		4.1	Understanding the organization and its context

2005		2013	
		4.1	
		4.2	Understanding the needs and expectations of interested parties
		4.2	
		4.2a	a)
		4.2b	b)
4.2	Establishing and managing the ISMS		
4.2.1	Establish the ISMS		
4.2.1			
4.2.1a		4.3	Determining the scope of the information security management system
		4.3	
		4.2a	a)
		4.2b	b)
		4.2c	c)
4.2.1b	b)	5.2	Policy
		5.2a	a)

2005		2013	
	1)	5.2b	b)
		5.1	Leadership and commitment
		5.1a	a)
	2)	5.2	Policy
		5.2c	c)
		5.2d	d)
	3)	5.1	Leadership and commitment
		5.1a	a)
	4)	6.1.2	Information security risk assessment
		6.1.2 a1	[1]
	5)	5.2	Policy
		5.2	
		5.2f	f)
		5.2g	g)

2005		2013	
4.2.1c 4.2.1d 4.2.1e	c) 1) 2) d) 1) 2) 3) 4) e) 1) 2) 3) 4)	6.1.1 6.1.2	<u>General &</u> <u>Information security risk assessment</u>
		6.1.1	a) b) c) a) b) 1) 2)

2005		2013	
		6.1.2	a) 1) 2) b) c) 1) 2) d) 1) 2) 3) e) 1) 2)
4.2.1f	f) 1) 2) 3) 4)	6.1.3	Information security risk treatment
		6.1.3 a	The organization **shall** define and apply an information security risk treatment process to: a)
		6.1.3 *	
4.2.1g	g)	6.1.3	Information security risk treatment

2005		2013	
		6.1.3 b	b)

2005		2013	
	h) manage… pr… res… al risk	6.1.3	Information security risk treatment
		6.1.3 f	f)
4.2.1i	i)		
4.2.1j	j)	6.1.3	Information security risk treatment

2005		2013	
	1) 2) 3)	6.1.3 c 6.1.3 d	c) d)

2005		2013	
4.2.2	Implement and operate the ISMS		
4.2.2a		6.1.3	Information security risk treatment

2005		2013	
	a)	6.1.3 e	e)
4.2.2b 4.2.2c	b) c)	8.3	Information security risk treatment
		8.3	
4.2.2d	d)	9.1	Monitoring, measurement, analysis and evaluation
		9.1a 9.1b	a) b)
4.2.2e	e)	7.2	7.2 Competence

2005		2013	
		7.2c	c)
		7.3	<u>Awareness</u>

2005		2013	
		7.3a 7.3b 7.3c	a) b) c)

2005		2013	
4.2.2f	f)	8.1	Operational planning and control
4.2.2.g	g)	7.1	Resources
		7.1	determine
4.2.2h	h)	8.1	Operational planning and control
		8.1	
4.2.3	Monitor and review the ISMS		

2005		2013	
4.2.3a	a)		
	1)	A16	Information security incident management
	2)		
	3)	9.1	Monitoring, measurement, analysis and evaluation
		9.1	
	4)	A16	Information security incident management
	5)		
4.2.3b 4.2.3c	b)	6.2	Information security objectives and plannings to achieve them
		6.2e	e)
		9.1	Monitoring, measurement, analysis and evaluation
	c)	9.1	e)
4.2.3d	d)	6.1.2	Information security risk assessments
		6.1.2 a2	a) 1)

2005		2013	
		8.2	Information security risk assessment
		8.2	
	1)	9.3	Management review

2005		2013	
	2) 3) 4) 5) 6)	9.3	a) b) c) 1) 2) 3) 4) d) e) f)

2005		2013	
	e)	9.2	Internal audit
		9.2	
	f)	4.3a 4.3b	Determining the scope of the information security management system
	g)	4.3a 4.3b	a) b)
		9.3	Management review
		9.3	g) h) i) 5) 6) 7) 8) j) k) l)
	h)	4.1	Understanding of the organization and its context

2005		2013	
		4.1	
4.2.4	Maintain and improve the ISMS		
4.2.4 4.2.4a	a)	10.2	Continual improvement
		10.2	
4.2.4b	b)	10.1	Nonconformity and corrective action
		10.1 c	c)
		10.2	Continual improvement
		10.2	
4.2.4c	c)	7.4	Communication

2005		2013	
		7.4	a) b) c) d) e)
4.2.4d	d)	9.3	Management Review
		9.3f	f)
4.3	Documentation requirements		
4.3.1	General		
4.3.1			
4.3.1a	a)	5.2	Policy
		5.2e	e)
		6.2	Information Security Objectives and planning to achieve them
		6.2e +	
4.3.1b	b)	4.3	Determining the scope of the information security management system
		4.3c+	
4.3.1c	c)	7.5 7.5.1	Documented Information General
		7.5.1	a) b)
4.3.1d	d)	6.1.2	Information Security Risk Assessment

2005		2013	
4.3.1e	e)	6.1.2 e2+	
		8.2	Information security risk assessment
		8.2+	
4.3.1f	f)	6.1.1	General (Actions to address risk and op.)
		6.1.1 e1	d) e) 1)
		6.1.3	Information security risk treatment
		6.1.3 e 6.1.3 f+	e)
4.3.1g	g)	9.1	Monitoring, measurement, analysis and evaluation
		9.1f+	
4.3.1h	h)	7.5 7.5.1	Documented Information General
		7.5.1	a) b)
		9.2	Internal audit
		9.2g	g)
		9.3	Management review
		9.3f+	
4.3.1i	i)	6.1.3	Information security risk treatment
		6.1.3 d	d)

2005		2013	
			about the information security risk treatment process
			Deleted
		7.5 7.5.1	Documented information General
		7.5.1 b+	1) 2) 3)
		7.5.2	Creating and updating
		7.5.2	b)
4.3.2	Control of documents		
4.3.2		7.5.3	Control of documented information
		7.5.3	a) b)
4.3.2a 4.3.2b	a) b)	7.5.2	Creating and updating
		7.5.2 c	c)
4.3.2c	c)	7.5.3	Control of documented information
		7.5.3 e	e)
4.3.2d	d)	7.5.3	Control of documented information
		7.5.3 a	

2005		2013	
			a)
4.3.2e	e)	7.5.3	Control of documented information
		7.5.3 d	d)
4.3.2f	f)	5.2	Policy
		5.2g	g)
		7.5.3	Control of documented information
		7.5.3 c 7.5.3 f	c) f)
4.3.2g	g)	7.5.3	Control of documented information
		7.5.3 f+ 7.5.3 f	
4.3.2h	h)	7.5.3	Control of documented information

2005		2013	
	i)	7.5.3 c	c)

2005		2013	
	j)	7.5.2	Creating and updating
		7.5.2 a	a)
4.3.3	Control of records		
4.3.3		9.2	Internal Audit
		9.2g	g)
		7.5.3	Control of documented information
		7.5.3 b	b)
		5.2	Policy
		5.2c	c)
		7.5.3	Control of documented information
		7.5.3 d	e)
		5.3	Organizational roles, responsibilities and authorities
		5.3a 5.3b	a) b)
		8.1	Operational planning and control
		8.1	

2005		2013	
		8.3	Information security risk treatment
		8.3	
5	Management responsibility		
5.1	Management commitment		
5.1		5.1	Leadership and commitment
		5.1h	
	a)	5.2	Policy
		5.2	
	b)	5.1	Leadership and commitment
		5.1a	a)
		6.2	Information security objectives and planning to achieve them
		6.2	
	c)	5.3	Organizational roles, responsibilities and authorities
		5.3	a) b)
		5.1	Leadership and commitment
		5.1f 5.1h	

2005		2013	
			f) h)
	d)	5.1	Leadership and commitment
		5.1d 5.1f 5.1g 5.1h	d) f) g) h)
		6.2	Information security objectives and planning to achieve them
		6.2d	d)
		7.4	Communication
		7.4	
	e)	5.1	Leadership and commitment
		5.1c	c)
	f)	6.1.2	Information security risk acceptance
		6.1.2 a1	a) 1)
	g) h)	5.1	Leadership and commitment

2005		2013	
			e)
			f)
			h)
5.2	Resource management		
5.2.1	Provision of resources		
5.2.1		7.1	Resources
	a)		
	b)		
	c)		
	d)		
	e)		
	f)		
5.2.2	Training, awareness and competence		
5.2.2		7.2	Competence
	a)	7.2	a)
	b)		b)
	c)		c)
	d)		d)
	e)		

2005		2013	
		7.3	Awareness
		7.3	a) b) c)
6	Internal ISMS audits		
6	a) b) c) d)	9.2	Internal audit
		9.2	a) 1) 2) b) c) d) e) f)
7	Management review of the ISMS		
7.1	General		
7.1		9.3	Management review

2005		2013	
		9.3	a) b) c) 1) 2) 3) 4) d) e) f)
7.2	Review input		
7.2	a) b) c) d) e) f) g) h) i)		
7.3	Review output		
7.3	a) b) c) 1) 2) 3) 4) 5) 6) d) e)		
8	ISMS improvement		
8.1	Continual improvement		
8.1		10.2	Continual improvement

2005		2013	
		10.2	
8.2	Corrective action	10.1	Nonconformity and corrective action
8.2	a) b) c) d) e) f)	10.1	a) 1) 2) b) 1) 2) 3) c) d) e) f) g)
8.3	Preventive action		
8.3	a) b) c) d) e)		

2005		2013	